INSTITUTE VLATACOM

vKDS

# vKDS - Vlatacom Key Distribution System

## System Description

Vlatacom Key Distribution System represents the component that strongly interacts with PKI and symmetrical key production system. Its product is final encapsulated key that besides key content contains certificates and could be used only in device for which is created and o nly by authorized person. Since encryption process security is based on used keys, the proposed Core Security Solution for ICT system gives basis for proper usage of text and file encryption devices, voice encryption devices, video-teleconferencing de- vices, transmission lines encryption devices and entire information system integral security.

## Key Features

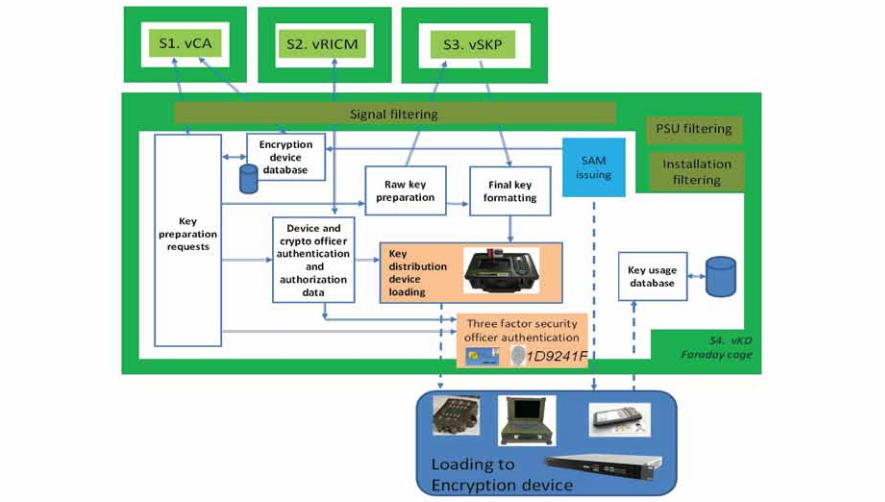
- Centralized key management system
- Compatible with Vlatacom Certification Authorities system vCA and Vlatacom Symmetrical Key Production System vSKP.
- Communication with vCA and vSKP by fiber optic lines running Transport Layer Security and Secure Shell Layer TLS/SSL protocols ensures maximal communication protection.
- Strong three factor authentication and authorization of all involved persons relayed on vCA system according to what I am, what I have and what I know principles.
- All devices in key management chain are authenticated by vCA
- Enables secure machine to machine communication
- Temper proof key distribution device with three factor crypto officer user authentication
- Key usage data base

## Supported Standards

- Key management according to X.509, PKIX (RFC5280) and PKCS#12
- Supported protocols for communication with CA: OCSP (RFC2560, RFC5019), CRLS (RFC4387), CMP (RFC4210 and RFC 4211). Certificate revocation lists according to RFC5280.
- Distributed keys originate from true random sequence that satisfies NIST SP 800-22A
- Keys are hashed according to NIST SHS PUB 180-4.
- Custom communication protocols, hash function and key management schemes are available on demand.

## System Architecture and Interfacing

Entire system is installed in electromagnetic eavesdropping safe environ- ment. Authorized security officer, which authentication and authorization data are certified by Vlatavom certification authority vCA initiates key preparation requests for specific encryption devices, which would be loaded to devices by specific crypto officers. According to these requests symmetrical key pro- duction system produces key in raw format. Keys are packed in final format ready to be loaded into temper safe key distribution devices. The keys are loaded to specific encryption devices at remote location in electromagnetic tents or faraday cages. Information about successful key loading to encryp- tion devices is stored into key distribution device and loaded keys are per- manently deleted from it which minimizes key compromising possibilities and ensures maximal security. The key distribution database is returned to vKDS cage and information about loading keys in crypto device is stored in key usage database.




## Key Benefits

- One centralized key distribution system for all encryption devices.
- Centralized key generation and key usage database ensures maximal security and control of entire encryption process
- Enables long term secure machine to machine communication

INSTITUTE VLATACOM

*Address:*
*Vlatacom d.o.o.*
*Milutina Milankovića 5*
*11070 Belgrade, Serbia*

*tel: +381 11 377 11 00*
*fax: +381 11 377 11 99*
*info@vlatacom.com*
*www.vlatacom.com*